Ministério da Educação
Universidade Federal de São Paulo
Instituto de Ciência e Tecnologia

Plano de Atividades Domiciliares Especiais (ADE)

Unidade Curricular: Teoria dos Números e Criptografia

Professor: Robson da Silva **Contato:** silva.robson@unifesp.br

Ano Letivo: 2020 **Semestre:** 1º

Carga horária total:

72 horas, sendo 8 já cumpridas presencialmente e 64 horas que serão cumpridas remotamente.

Turmas: /

Plataforma de acesso ao curso: *Google Classroom.*

Objetivos:

- Familiarizar o aluno com conceitos básicos de Teoria dos Números. Introduzir os conceitos de Criptografia fazendo a relação entre a base matemática teórica com a parte computacional necessária para implementações numéricas. Discussão sobre a necessidade da sociedade contemporânea de proteção de dados. Compreender os aspectos interdisciplinares do assunto.
- Ao final da unidade curricular o aluno deverá ser capaz de reconhecer e resolver problemas relacionados aos números inteiros e suas propriedades básicas. O aluno deve compreender os conceitos de criptografia fazendo a relação entre a base matemática teórica com a parte computacional necessária para implementações numéricas. Além disso, o aluno deve saber debater sobre a necessidade da sociedade contemporânea de proteção de dados. O aluno deve compreender os aspectos interdisciplinares de Matemática, Computação e Humanidades, envolvidos no assunto e ter uma visão maior de como fazer relações semelhantes com outros temas estudados no curso.

Conteúdo Programático e Cronograma: vide tabela a seguir.

Semana	Conteúdo	Práticas Pedagógicas	Carga Horária
1 (03/08 a 09/08)	Revisão: divisibilidade, Teorema Fundamental da Aritmética, número primos.	Atividade assíncrona: conteúdo digital	2,5
		Atividade síncrona: plantão de dúvidas	1,0
		Atividade assíncrona: atividade avaliativa	2,3
2 (10/08 a 16/08)	MMC, representação de inteiros	Atividade assíncrona: conteúdo digital	2,5
		Atividade síncrona: plantão de dúvidas	1,0
		Atividade assíncrona: atividade avaliativa	2,3
3 (17/08 a 23/08)	Equações diofantinas. Fatoração do fatorial.	Atividade assíncrona: conteúdo digital	2,5
		Atividade síncrona: plantão de dúvidas	1,0
		Atividade assíncrona: atividade avaliativa	2,3
4 (24/08 a 30/08)	Congruência. Os inteiros módulo m. Congruência linear.	Atividade assíncrona: conteúdo digital	2,5
		Atividade síncrona: plantão de dúvidas	1,0
		Atividade assíncrona: atividade avaliativa	2,3
5 (31/08 a 06/09)	Teorema Chinês dos restos. Teoremas de Euler, Fermat e Wilson	Atividade assíncrona: conteúdo digital	2,5
		Atividade síncrona: plantão de dúvidas	1,0
		Atividade assíncrona: atividade avaliativa	2,3
6 (07/09 a 13/09)	Funções aritméticas.	Atividade assíncrona: conteúdo digital	2,5
		Atividade síncrona: plantão de dúvidas	1,0
		Atividade assíncrona: atividade avaliativa	2,3
7 (14/09 a 20/09)	Funções aritméticas. Produto de Dirichlet.	Atividade assíncrona: conteúdo digital	2,5
		Atividade síncrona: plantão de dúvidas	1,0
		Atividade assíncrona: atividade avaliativa	2,3
8 (21/09 a 27/09)	Resíduos quadráticos. Símbolo de Legendre.	Atividade assíncrona: conteúdo digital	2,5
		Atividade síncrona: plantão de dúvidas	1,0
		Atividade assíncrona: atividade avaliativa	2,3
9 (28/09 a 04/10)	Resíduos quadráticos. Lei da Reciprocidade Quadrática.	Atividade assíncrona: conteúdo digital	2,5
		Atividade síncrona: plantão de dúvidas	1,0
		Atividade assíncrona: atividade avaliativa	2,3
10 (05/10 a 11/10)	Raízes primitivas.	Atividade assíncrona: conteúdo digital	2,5
		Atividade síncrona: plantão de dúvidas	1,0
		Atividade assíncrona: atividade avaliativa	2,3
11 (11/10 a 19/10)	Criptografia.	Atividade assíncrona: conteúdo digital	2,5
		Atividade síncrona: plantão de dúvidas	1,0
		Atividade assíncrona: atividade avaliativa	2,3

Metodologia de Ensino Utilizada:

- Atividades síncronas:
  (i) Discussão do conteúdo da semana;
  (ii) Plantão de dúvidas.
- Atividades assíncronas:
  (i) Disponibilização de conteúdo digital (videoaulas, textos, listas de exercícios para aprendizagem e fixação de conceitos, etc.).
  (ii) Atividades avaliativas a serem entregues semanalmente pelos alunos.

Metodologia de Avaliação:

As alunas e os alunos serão avaliados continuamente por meio de atividades semanais, que poderão ser realizadas diretamente na plataforma ou de forma manuscrita. Neste último caso, a atividade deverá ser digitalizada em um arquivo PDF e a ser enviado ao professor. A forma de entrega de cada atividade será definida pelo docente no momento de sua disponibilização na plataforma. Cada atividade deverá ser entregue após 7 (sete) dias da divulgação da mesma.

A frequência no curso será contabilizada por meio da entrega de cada uma das atividades semanais. As alunas e os alunos que enfrentem qualquer tipo de problema que acarrete a não entrega da atividade no prazo estipulado, deverão entrar em contato com o docente com a maior brevidade possível. Cada atividade valerá de 0 (zero) a 10 (dez) pontos, e, ao término do semestre, será computada a média aritmética (M) das notas das atividades.

Alunas e alunos com menos do que 75% de frequência terão o conceito “Não Cumprido”. Caso tenha pelo menos 75% de frequência (ou seja, caso tenha entregue pelo menos 9 das 11 atividades semanais) e

- se M >= 6,0 (seis), a aluna ou o aluno atingirá o conceito “Cumprido”.
- se M < 6,0 (seis), a aluna ou o aluno atingirá o conceito “Não Cumprido”.

Bibliografia básica e complementar:

Básica:

1. da SILVA, R. Notas de aula disponíveis em https://drive.google.com/file/d/1mMdMJJFbytNrOm1zwU547eqACMMPpUP6/view
2. MARTINEZ, F. B.; MOREIRA, C. G.; SALDANHA, N.; TENGAN, E. Teoria dos números, um passeio com primos e outros números familiares pelo mundo inteiro. 2ª ed. Rio de Janeiro: IMPA, 2011.
3. SANTOS, J. P. O. Introdução à teoria dos números. 3ª ed. Rio de Janeiro: SBM-IMPA, 2009.

Complementar:

1. COUTINHO, S. C. Números inteiros e criptografia RSA. 2ª ed. Rio de Janeiro: SBM-IMPA, 2005
2. DAVENPORT, H. The higher arithmetic: an introduction to the theory of numbers. 8ª ed. Cambridge: Cambridge Univeristy Press, 2008.
3. HARDY, G. H.; WRIGHT, E. M. An introduction to the theory of numbers. 6ª ed. Oxford: Oxford University Press, 2008.
4. HEFEZ, A. Elementos da aritmética. 2ª ed. Rio de Janeiro: SBM-IMPA, 2006.

Av. Cesare Mansueto Giulio Lattes, 1201. Parque Tecnológico.
Eugênio de Melo – CEP: 12247-014 – São José dos Campos, SP
Telefone: (12) 3924-9503 / 9547